CyberTalents Challenges

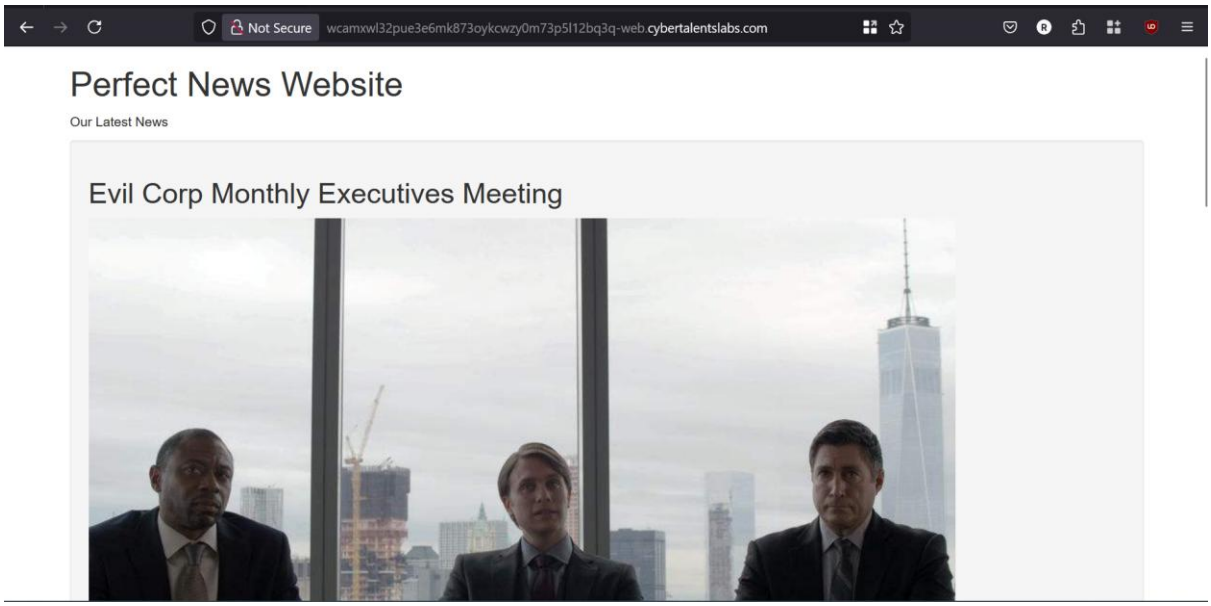
Web Security – who is admin – level medium

Author: levith4n

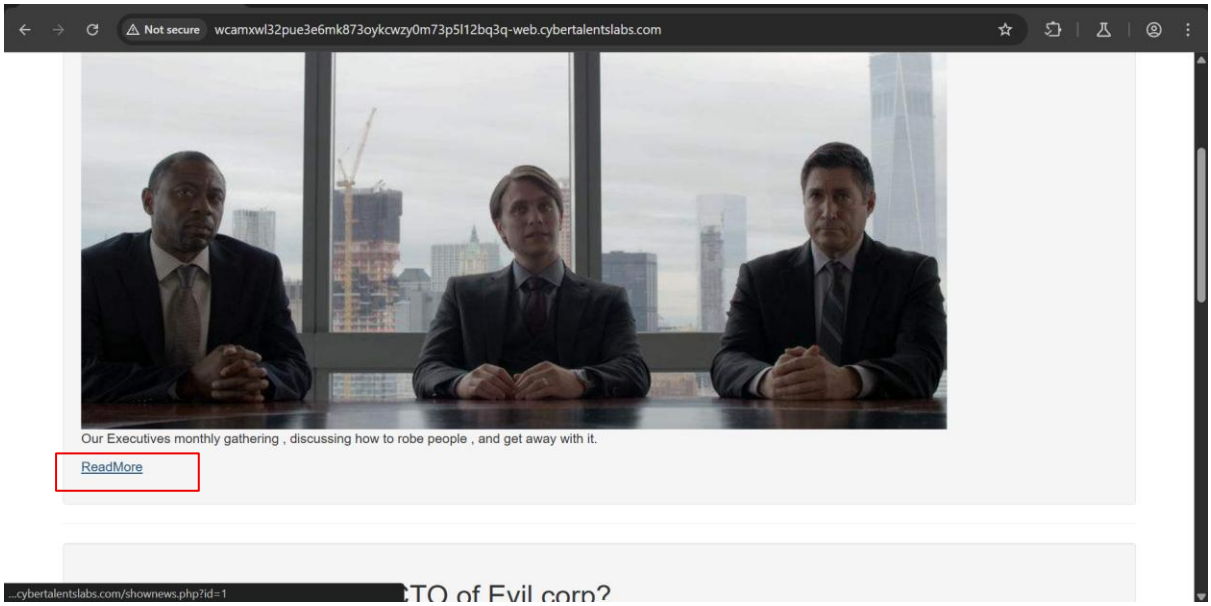
Description:

Your mission is to know who's the admin running this website by knowing his email.

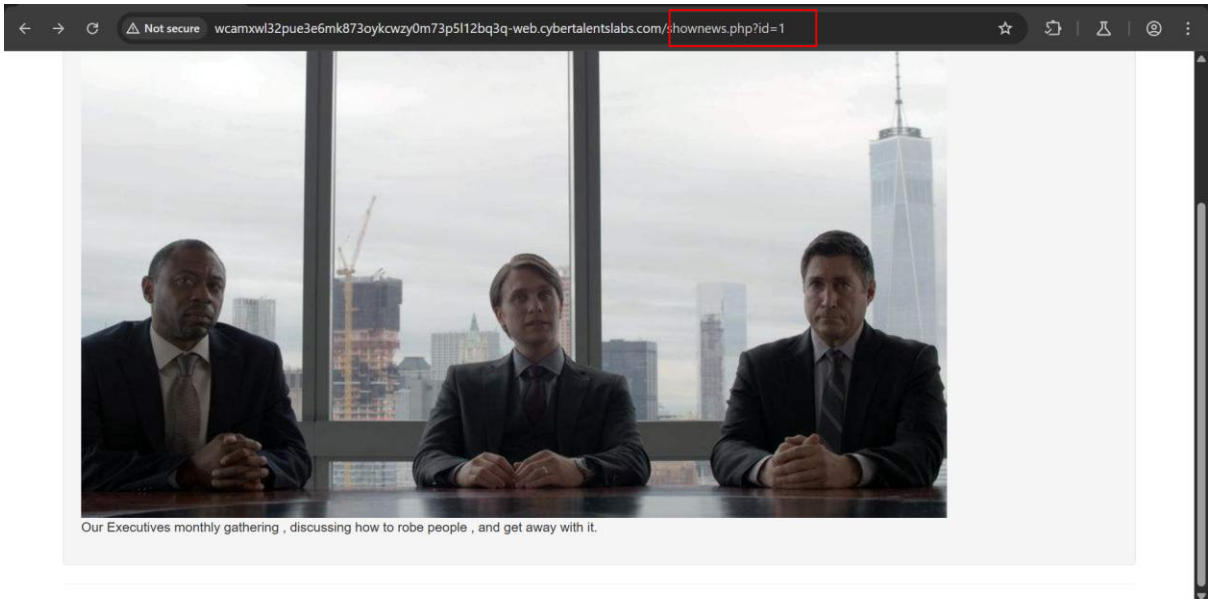
Pertama, ini adalah tampilan utama dari website target.



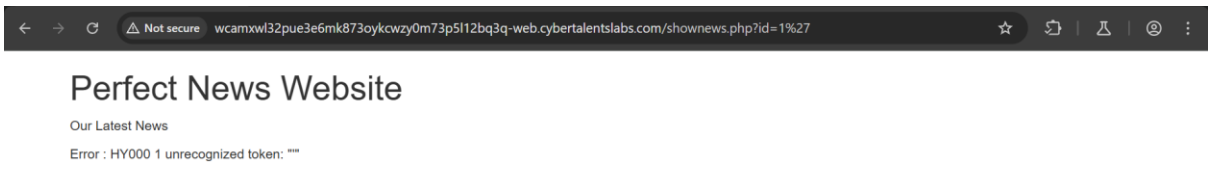
Kemudian saat meng-*scroll*, saya menemukan sebuah tautan **ReadMore**.



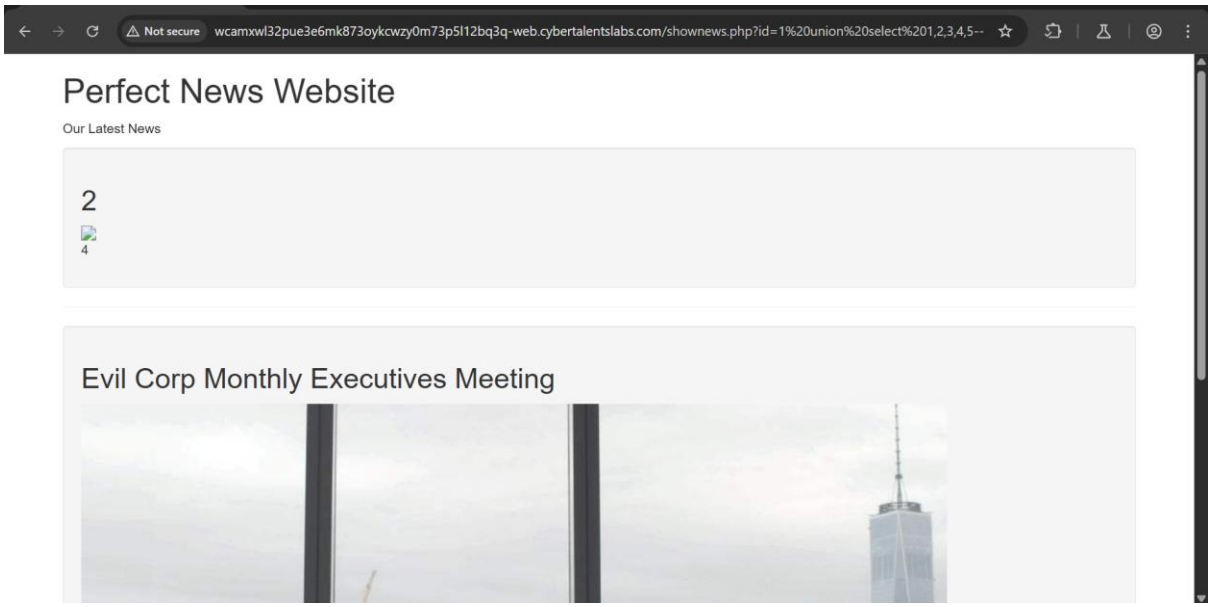
Setelah ditekan, tombol tersebut mengarahkan ke halaman seperti gambar di bawah ini. Tidak ada hal menarik pada halaman ini, kecuali parameter **id**.



Saya mencoba melakukan *SQL Injection* dengan menambahkan tanda petik satu (‘) pada parameter tersebut dan mendapatkan pesan *error*, pesan error ini berasal dari **DBMS SQLite**.



Selanjutnya, saya mencoba untuk melakukan *Union Injection* dan berhasil menentukan jumlah kolom pada table yang terhubung dengan website, yaitu **5**, serta kolom yang ditampilkan hanya lah 2, 3 (gambar) dan 4.



Selanjutnya saya mencoba mengekstrak table dan column pada database website ini.

|*Payload*: **union select 1, sql, 3, 4, 5 from sqlite_master where type=”table”-- -**

Dengan kolom **sql** pada table **sqlite_master** kita mencoba mengekstrak struktur pembuatan table-tabel pada database yang terhubung dengan website ini. Seperti yang bisa kita lihat pada gambar, kita menemukan sebuah table dengan nama **nxf8_users** yang didalamnya terdapat kolom **name, email, password** dan **role**.

Terakhir, saya mencoba untuk mengekstrak email dari role admin dan berhasil mendapatkan email admin.

|*Payload:* **union select 1, email,3 ,4, 5 from nxf8_users where role=”admin”-- -**